Information security processing system and method for electric business

Publication number: CN1373423 (A)
Publication date: 2002-10-09
Inventor(s): CHEN ZHOGUANG [CN]; GONG ZHIHUI [CN]
Applicant(s): LIMING NETWORK CO LTD [CN]
Classification:
- international: ***G06F12/08;*** **G06F12/08**; (IPC1-7): G06F12/08
- European:
Application number: CN20011007620 20010228
Priority number(s): CN20011007620 20010228

Also published as:
CN1206595 (C)

Abstract of **CN 1373423 (A)**

A high-security system for processing E-business information has an authentication center CA connecting with more trade systems and providing security service authentication and a CA data buffer poolconnected to said authentication cencer. The trade credit information in CA data buffer poll is synchronized with the relative data in authentication center. Its advantages are high performance of trade system and high versatility of PKI system.

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 12/08

[12]发明专利申请公开说明书

[21]申请号 01107620.8

[43]公开日 2002年10月9日

[11]公开号 CN 1373423A

[22]申请日 2001.2.28 [21]申请号 01107620.8

[71]申请人 黎明网络有限公司
地址 518031 广东省深圳市福田区深南中路统建楼一栋15－20层
[72]发明人 陈朝光 龚智辉

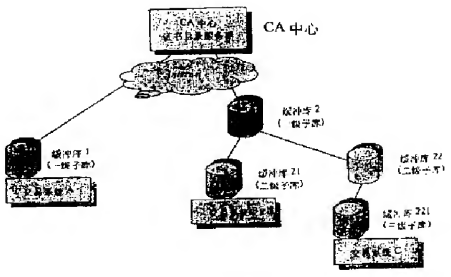
[74]专利代理机构 深圳市顺天达专利商标代理有限公司
代理人 郭伟刚

权利要求书3页 说明书10页 附图页数4页

[54]发明名称 电子商务信息安全处理系统及其方法

[57]摘要

一种电子商务信息安全处理系统，包括可与多个交易系统连接并 提供安全服务认证的CA认证中心，通过一定方式与所述CA认证中 心连接的CA数据缓冲库，CA数据缓冲库中的交易信用信息与CA认证中心的相关数据保持同步。由于采用同步机制，解决了同CA中心在线通信所带来的性能上的损耗，提高了交易系统的性能；也解决 了与Internet断开连接的交易系统的PKI使用和校验问题；还因采用 构造系统证书库及多级同步机制的方法，增强了PKI体制的通用性。



ISSN1008-4274

知识产权出版社出版

01.03.12

权 利 要 求 书

1、一种电子商务信息安全处理系统，包括可与多个交易系统连接并提供安全服务认证的 CA 认证中心，其特征在于，还包括通过一定方式与所述 CA 认证中心连接的 CA 数据缓冲库，所述 CA 数据缓冲库中的交易信用信息与所述 CA 认证中心的相关数据保持同步。

2、根据权利要求 1 所述电子商务信息安全处理系统，其特征在于，所述 CA 数据缓冲库的部分或全部存储在所述交易系统上。

3、根据权利要求 1 所述电子商务信息安全处理系统，其特征在于，所述 CA 数据缓冲库的部分或全部存储在与所述交易系统连接的近端设备上。

4、根据权利要求 1-3 所述电子商务信息安全处理系统，其特征在于，所述 CA 数据缓冲库包含的 CA 认证信息包括 CA 中心的根证书、证书吊销列表以及系统本身的和所属用户的电子证书。

5、根据权利要求 1 所述电子商务信息安全处理系统，其特征在于，所述 CA 数据缓冲库中的交易信息是通过交易系统定时下载或实时读取所述 CA 中心的相关数据来实现其同步的 。

6、根据权利要求 1 所述电子商务信息安全处理系统，其特征在于，所述 CA 数据缓冲库为多层结构，其中，每一层 CA 数据库均为其

上一层CA数据缓冲缓冲库的子集,且每一层CA数据库中的交易信用信息与上一层CA数据缓冲库的信息保持同步,并最终与CA中心的交易信用信息保持同步。

7、一种电子商务信息安全处理方法，其特征在于，包括以下步骤:

通过同步机制将CA中心中与交易系统进行安全处理时所需的交易信用信息存贮到CA数据缓冲库中；

将所述CA数据缓冲库的交易信用信息与所述CA中心对应信息保持同步；

交易系统从CA数据缓冲库读取交易信用信息。

8、根据权利要求7所述电子商务信息安全处理方法，其特征在于，还包括对来自所述CA中心的交易信用信息进行筛选后有选择地保存的步骤，所述筛选是从中选择出包括CA中心的根证书、证书吊销列表(CRL)和与本系统相关的证书的信息。

9、根据权利要求7所述电子商务信息安全处理方法，其特征在于，还包括检测到所述CA数据缓冲库中交易信用信息受到破坏时进行自动恢复的步骤。

10、根据权利要求7所述电子商务信息安全处理方法，其特征在于，所述CA安全认证信息包括CA中心的根证书、证书吊销列表(CRL)和与本系统相关的证书。

11、根据权利要求 7 所述电子商务信息安全处理方法，其特征在于，所述同步机制是指定时下载或通过软件定时读取所述 CA 中心中交易信用信息实现。

说 明 书

电子商务信息安全处理系统及其方法

本发明涉及网络交易安全技术，具体涉及一种电子商务信息安全处理系统及其方法。

近年来，信息安全成为极度热门的话题 ，特别是电子商务的兴起使信息安全问题更为突出。人们从现实世界进入电子世界，通过网络进行交流和商业活动，面临的最大问题是如何建立相互之间的信任关系以及如何保证信息的真实性、完整性、机密性和不可否认性。加密技术是解决这一系列问题的技术基础。加密数据是算法、密钥和明文的数学运算结果，现代密码学中，利用可公开的、标准的算法，通过对密钥的保护来达到数据的加密目的，这种做法称为基于密钥的安全性。若数据的加解密使用相同的密钥，则称这种密钥为对称密钥；若加解密采用不同的密钥，则称为非对称密钥，由于非对称密钥的加密密钥和解密密钥无法相互推算出来，因此，加密密钥可以公开，因此也称为公开密钥。公开密钥基础设施(Public Key Infrastructure ，简称 PKI)技术正是使用了非对称密钥的技术。P KI 提供网上管理关系的技术，其基本机制是：定义及建立身份、认证及授权的技术，然后分发、交换这些技术，在企业与网络之间解释及管理这些信息。PKI 的任务是在所有参与者之间建立平等的信誉关系，保证企业电子在线

交易系统的安全。

依据 PKI 体制的工作机理，交易双方事先须有证书认证机构（简称 CA 中心）颁发的证书和相对应的私钥。在交易时，需要对方的证书，发送者从对方的证书中获得公钥用以加密打算传输的数据，同时可以用自己的私钥对数据进行签名；接收者则利用自己的私钥解开对方利用自己证书中公钥加密的数据，同时需要知道对方的证书来用以验证对方的电子签名。这样交易双方的证书均是公正的第三方权威认证机构所颁发，交易者通过对权威认证机构来达到对交易对方信任的目的。进行这种三方认证，交易者需要从 CA 中心获取交易对方的证书，同时还需要对对方送过来的证书进行校验以确定他的有效性。

当前业界的普遍做法是采用交易双方直接同 CA 中心建立连接的方式来进行。如图 1 所示，交易者甲需要同交易者乙进行业务往来时，需要实时向 CA 中心获取交易者乙的电子证书，检验电子证书的有效性，并利用该证书进行数据的加密工作。若需要电子签名，甲会利用自己的私钥对数据进行签名。乙在收到甲的数据后，利用自身的私钥进行解密。若有甲的电子签名，则乙通过从 CA 中心获取甲的电子证书，CA 中心的证书和 CA 中心颁发的证书吊销列表进行甲的电子签名的校验工作。乙向甲发送数据的流程与上同。

上述传统做法存在着缺陷具体表现在：首先，进行交易的双方均需同 CA 中心直接通过 Internet 连接，交易会受网络传输速度和无法预料的网络故障的影响，由于进行交易的双方均需同 CA 中心直接通

过 Internet 连接，对交易者环境要求较为苛刻，使用方式也太复杂，很大程度约束了基于 PKI 信息安全技术的交易系统的使用和推广；其次，每次涉及信息安全的交易均需同 CA 中心建立连接，获取所需数据，这会使交易系统的资源造成浪费。

本发明的目的在于，提供一种电子商务信息安全处理系统，通过采用构造一级或多级 CA 数据缓冲库，提高 PKI 体制的技能，以保证采用 PKI 机制的交易本身的信息安全。

本发明的另一目的是提供一种电子商务信息安全处理方法，通过构造 CA 数据缓冲库的方法，克服现有集中式的系统交易信用认证库存在的认证过程耗时长、特殊情况下无法实现信用认证的缺点，使得在保证整个系统交易安全的前提下，系统交易信用的认证更具有可实现性，使得信用认证不再成为电子商务的信息安全领域的瓶颈。

本发明的目的是这样实现的，构造一种电子商务信息安全处理系统，包括可与多个交易系统连接并提供安全服务认证的CA认证中心，其特征在于，还包括通过一定方式与所述 CA 认证中心连接的 CA 数据缓冲库，所述 CA 数据缓冲库中的交易信用信息与所述 CA 认证中心的相关数据保持同步。

在按照本发明提供的电子商务信息安全处理系统中，所述 CA 数据缓冲库的部分或全部存储在所述交易系统上。

在按照本发明提供的电子商务信息安全处理系统中，所述 CA 数

据缓冲库的部分或全部存储在与所述交易系统连接的近端设备上。

在按照本发明提供的电子商务信息安全处理系统中，所述 CA 数据缓冲库包含的 CA 认证信息包括 CA 中心的根证书、证书吊销列表以及系统本身的和所属用户的电子证书。

在按照本发明提供的电子商务信息安全处理系统中，所述 CA 数据缓冲库中的交易信息是通过交易系统定时下载或实时读取所述 CA 中心的相关数据来实现其同步的 。

在按照本发明提供的电子商务信息安全处理系统中，所述 CA 数据缓冲库为多层结构,其中,每一层 CA 数据库均为其上一层 CA 数据缓冲缓冲库的子集,且每一层 CA 数据库中的交易信用信息与上一层 CA 数据缓冲库的信息保持同步,并最终与 CA 中心的交易信用信息保持同步。

本发明的另一个目的是这样实现的，构造一种电子商务信息安全处理方法，其特征在于，包括以下步骤：

通过同步机制将 CA 中心中与交易系统进行安全处理时所需的交易信用信息存贮到 CA 数据缓冲库中；

将所述 CA 数据缓冲库的交易信用信息与所述 CA 中心对应信息保持同步；

交易系统从 CA 数据缓冲库读取交易信用信息。

在按照本发明提供的电子商务信息安全处理方法中，还包括对来

自所述 CA 中心的交易信用信息进行筛选后有选择地保存的步骤，所述筛选是从中选择出包括 CA 中心的根证书、证书吊销列表(CRL)和与本系统相关的证书的信息。

在按照本发明提供的电子商务信息安全处理方法中，还包括检测到所述CA数据缓冲库中交易信用信息受到破坏时进行自动恢复的步骤。

在按照本发明提供的电子商务信息安全处理方法中，所述 CA 安全认证信息包括 CA 中心的根证书、证书吊销列表(CRL)和与本系统相关的证书。

在按照本发明提供的电子商务信息安全处理方法中，所述同步机制是指定时下载或通过软件定时读取所述CA中心中交易信用信息实现。

实施本发明提供的电子商务信息安全处理系统及其方法，具有以下优点：1）同步机制的采用，解决了同 CA 中心在线通信所带来的性能上的损耗，大大提高了交易系统的性能；2）解决了复杂环境，如一些为保证安全，防止受到非法攻击，而与 Internet 断开连接的交易系统的 PKI 使用和校验问题；3）采用构造系统证书库及多级同步机制的方法，增强了 PKI 体制的通用性，为 PKI 体制在电子商务交易中的推广提供了一条新的途径。

下面结合附图和实施例，对本发明的系统和方法作进一步说明，附图中：

图 1 是现有技术中交易双方与 CA 认证中心之间的关系示意图；

图 2 是按照本发明系统构造的电子商务信息安全处理系统的逻辑关系示意图，

图 3 是按照本发明系统和方法的基本交易过程的示意图；

图 4 是按照本发明系统和方法构造的可用于交易平台的交易系统的结构示意图；

图 5 是按照本发明系统和方法构造的可形成多级缓冲库系统的拓扑结构示意图。

如图 2 所示，按照本发明提供的电子商务信息安全处理系统，包括 CA 认证中心、通过一定方式与所述 CA 认证中心连接的 CA 数据缓冲库、可按一定方式保持所述 CA 数据缓冲库中的数据与所述 CA 认证中心相关数据保持一致的同步机制，用户不直接与 CA 认证中心进行电子商务信息处理活动，而是通过与 CA 认证中心的信息保持一致的 CA 数据缓冲库进行商务信息处理活动。CA 数据缓冲库可根据网络的需要在本地形成一级或多级 CA 数据缓冲库，使用者通过设立在本地的 CA 数据缓冲库进行电子商务信息处理活动。。

所述系统中的 CA 数据缓冲库包含的 CA 认证信息包括 CA 中心的根证书、证书吊销列表以及系统本身的和所属用户的电子证书。所述同步机制是指数据缓冲库通过定时下载或通过软件实现实时或定时读取 CA 中心的数据，以保证与 CA 中心的信息即时保持一致。

在图3所示的按照本发明提供的处理系统的一个实例中，商家甲、乙进行电子商务的交易活动时，需要进行安全的电子交易，采用的是基于证书的PKI技术。具体包括以下步骤：

1）商家甲、乙作为交易的双方，通过预定的同步机制，如定时下载或依靠软件实现实时或定时读取等方法从CA中心获取认证信息：同步机制实时或定时地检测本地的当前认证信息状态，同时读取CA中心目录服务器数据的当前状态，并将二者进行比较以确定是否需要进行数据的更新；一旦监测到交易系统中的CA认证信息需要进行更新，则根据本交易系统的业务要求，将需要进行更新的、该交易系统进行安全处理时所需要的CA认证信息，如系统所需要的客户证书、CA中心根证书、证书吊销列表以及所属用户所需要的电子证书等数据，从CA中心下载或读取并保存在本地的CA数据缓冲库中，同时对本地的当前认证信息状态进行修改以达到信息同步。

2）假设商家甲作为交易的发起者或启动者，则数据安全流程如以下3）、4）所述；

3）商家甲的交易系统读取本地的CA数据缓冲库，进行信息的安全处理和校验工作。信息的安全性通过以下两种处理方式来达到：一是通过对数据的加密来实现信息的保密性。甲可以从CA数据缓冲库取出商家乙的证书，利用其所含公钥进行数据加密；二是通过电子签名来实现信息的完整性、不可否认性和不可篡改，这要通过发送者的电子签名来解决。本例中，甲利用自己证书对应的私钥进行电子签名；

4）商家乙获得数据后，对信息进行处理和还原并进行相关的校验工作。对于加密的数据，乙可以以自身证书对应的私钥进行数据解密；对于带有电子签名的数据，乙首先需从缓冲库中取出甲的证书、CA中心根证书和吊销列表，利用根证书和证书吊销列表来验证甲证书的有效性，验证通过后再从该有效的电子证书中取出其所含公钥来校验甲的电子签名是否有效；

5） 一旦同步机制检测到所述信息安全系统遭到破坏，如出现线路故障等突然因素，此时系统的同步工作将无法进行，同步机制会给出相应的故障提示以提醒系统管理员及时把系统恢复到正常。但甲乙之间的交易仍然得以正常进行，这就避免了传统做法中交易者一旦同 CA 中心断开则交易无法进行的缺陷。不过在同步机制停止工作的时间内，甲乙交易系统所保持的数据是同步机制遭到破坏时的数据，在此期间 CA 中心的数据更新将无法被交易系统所获知。同步机制不断监测线路，一旦发现线路恢复， 同步机制自动恢复运转，进行相应的数据同步和更新，并向系统管理员递交系统恢复工作的提示或报告。

按照本发明提供的商务信息交易系统中，可以应用在电子商务交易平台上，在具有交易平台的电子商务交易系统中，交易者可以利用交易平台进行电子商务的交易活动，而没有同CA中心建立连接关系，从物理连接上同 CA 中心断开，他们的 CA 数据是靠从交易平台的证书库中的同步认证信息获取的。

具体流程如图 4 所示：首先，交易平台连接到 CA 中心，进行认

证信息的同步工作并存贮在交易平台的CA数据缓冲库中，通过同步机制保持即时更新，使交易平台上的CA 数据缓冲库成为CA中心认证信息库的子集，并使其中的交易信用信息与CA中心的交易信用信息同步；交易双方甲、乙通过同步机制，从交易平台的CA数据缓冲库中同步交易信用信息，并保存在本交易系统的CA数据缓冲子库中，通过同步程序保持即时更新，各交易系统的CA数据缓冲子库中的信息与交易平台的 CA 数据缓冲库中的信息保持同步，并实质上是与CA中心的信息保持同步。

按照本发明提供的商务信息交易系还可用于形成多级CA缓冲库库，如图5所示，该系统中的三个交易参与者A,B,C分别使用不同级的同步方式实现CA数据的同步工作。不同级别的同步的信息各不相同，同一级别同步的信息也根据各自系统需要的差异和筛选条件的不同而略有不同。各级交易系统缓冲库中的CA认证信息分别与其上一级CA数据缓冲库中的认证信息保持同步，并实质上与CA中心的认证信息保持同步。

CA数据缓冲库可以满足CA证书库的基本目录服务功能，通过同CA中心的同步机制，拥有完备的证书有效性等校验信息，满足系统中的证书查询、校验等工作系统内部对证书库的使用采用的是多级缓冲机制，在满足CA体系的安全性基础上优化了系统处理证书查询和有效性校验的性能。它解决了现有技术中存在的证书目录服务必须同CA证书目录服务器有物理上的连接，并且每次涉及CA安全校验均需使用CA目录服务器问题，从而导致系统性能大大降低的问题。

因为用户和商家的业务系统可以直接地从交易终端 CA 数据缓冲库中读取 CA 的相关数据，进行信息安全的校验和处理工作。从而在保证信息安全性丝毫不受影响的前提下，免去了同 CA 中心直接连接获取数据所带来的一系列问题。

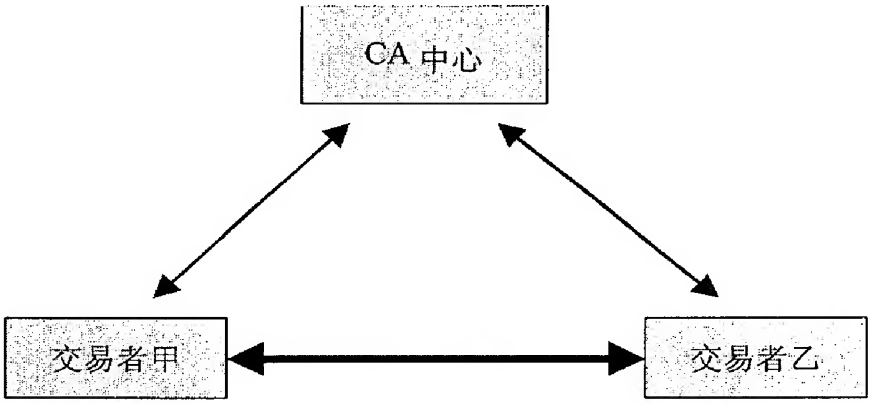


图 1

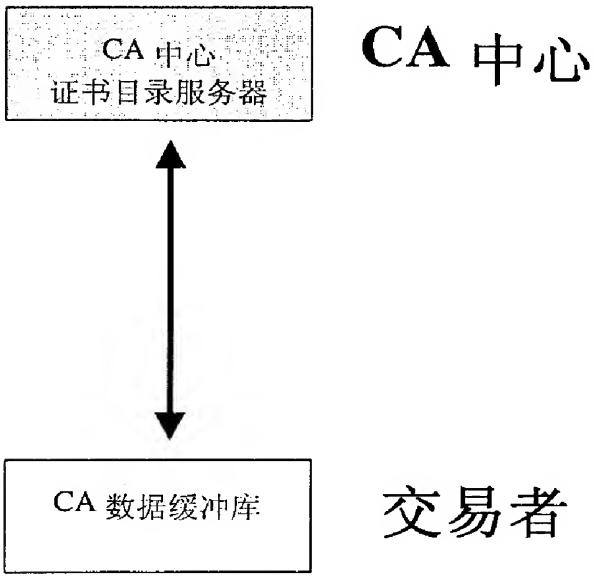


图 2

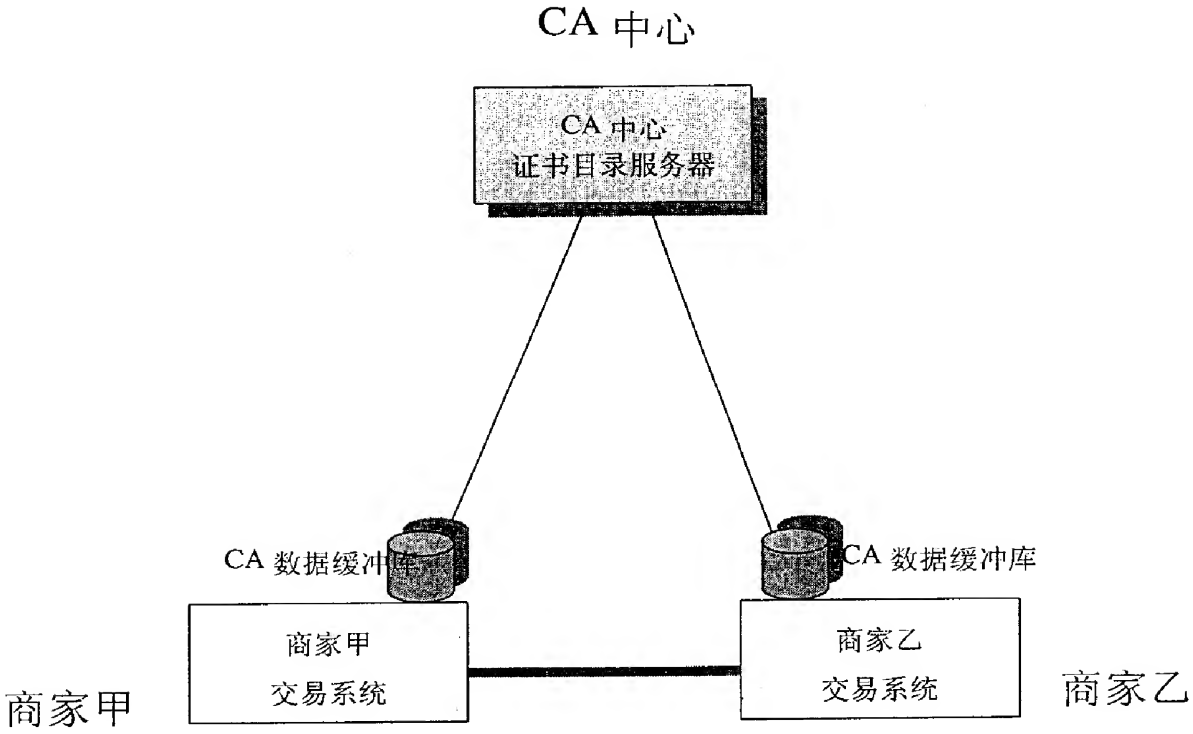


图 3

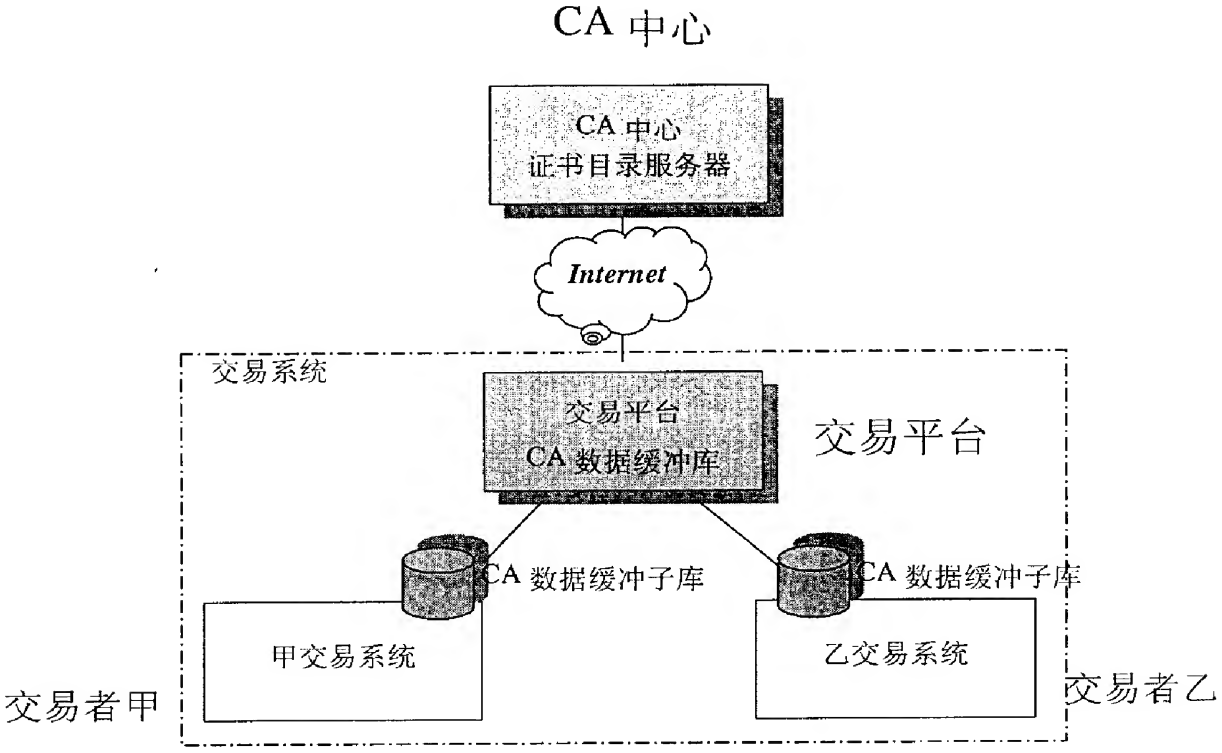

CA 中心
CA 中心
证书目录服务器
Internet
交易系统
交易平台
CA 数据缓冲库
交易平台
CA 数据缓冲子库
CA 数据缓冲子库
甲交易系统
乙交易系统
交易者甲
交易者乙

图 4

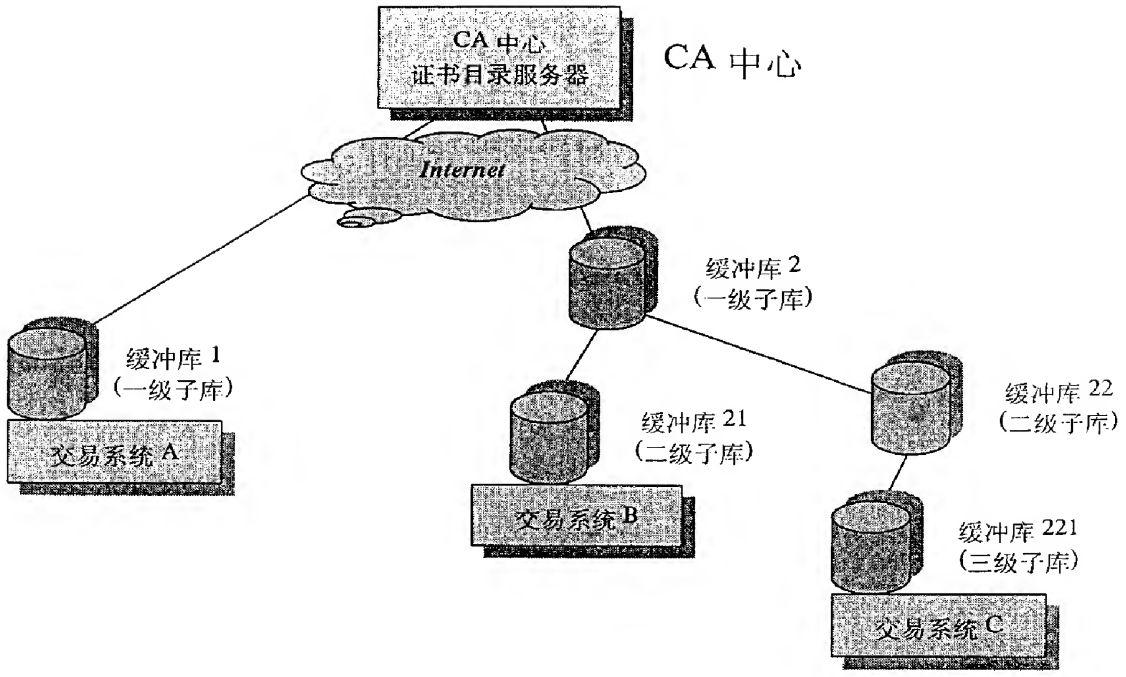

CA 中心
证书目录服务器
CA 中心
Internet
缓冲库 2
(一级子库)
缓冲库 1
(一级子库)
缓冲库 22
(二级子库)
缓冲库 21
(二级子库)
交易系统 A
交易系统 B
缓冲库 221
(三级子库)
交易系统 C

图 5